AMENDMENT AND PRESENTATION OF CLAIMS

Please replace all prior claims in the present application with the following claims.

1. (Previously Presented) A network system providing a virtual private network (VPN), said network system comprising:

one or more egress routers having connections to an access network including an access link, wherein said one or more egress routers transmit intra-VPN traffic to a destination host belonging to the VPN from sources within the VPN within a first access network logical connection for intra-VPN traffic and all extra-VPN traffic to the destination host from sources outside the VPN within a second access network logical connection for extra-VPN traffic, separate from the first access network logical connection, wherein intra-VPN traffic is given precedence over extra-VPN traffic by assigning a higher priority to the first access network logical connection; and

a plurality of ingress routers coupled to the one or more egress routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic, such that the intra-VPN traffic and the extra-VPN traffic are logically separated into different paths, whereby denial of service attacks on said access link originating from sources outside the VPN are prevented.

2. (Previously Presented) The network system of Claim 1, wherein the at least one of the plurality of ingress routers or the at least one of the one or more egress routers logically partitions intra-VPN traffic and extra-VPN traffic using a differentiated services protocol to mark correspondingly the intra-VPN traffic and the extra-VPN traffic.

3. (Previously Presented) The network system of Claim 1, and further comprising a plurality of customer premises equipment (CPE) edge routers each coupled to a respective one of said plurality of ingress routers.

4. (Currently Amended) The network system of Claim 1, and further comprising the access network, and a customer premises equipment (CPE) edge router to the access link.

5. (Canceled)

6. (Currently Amended) The network system of Claim ~~5~~ 4, said CPE edge router having a physical port coupled to said access link, said physical port implementing a first logical port for intra-VPN traffic and a second logical port for extra-VPN traffic.

7. (Currently Amended) The network system of Claim 1, wherein at least one of said plurality of ingress routers implements a plurality of tunnels that logically partition intra-VPN and extra-VPN traffic, and wherein said one or more egress routers provide a plurality of different qualities of services to said intra-VPN traffic.

8. (Canceled)

9. (Previously Presented) A network system, comprising:

an access network having an access link to a destination host belonging to a virtual private network (VPN), wherein said access network supports a first logical connection for intra-VPN traffic from sources within the VPN and a second logical connection for extra-VPN

traffic from sources outside the VPN, wherein intra-VPN traffic is given precedence over extra-VPN traffic by assigning a higher priority to the first logical connection;

one or more egress routers having connections to the access network, wherein said one or more egress routers transmit intra-VPN traffic to the destination host via the first logical connection and all extra-VPN traffic to the destination host via the second logical connection; and

a plurality of ingress routers coupled to the one or more egress routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic, such that intra-VPN traffic and extra-VPN traffic are logically separated into different paths, whereby denial of service attacks on said access link originating from sources outside the VPN are prevented.

10. (Previously Presented) The network system of Claim 9, wherein the at least one of the plurality of ingress routers or the at least one of the one or more egress routers logically partitions the intra-VPN traffic and the extra-VPN traffic using a differentiated services protocol to mark correspondingly the intra-VPN traffic and the extra-VPN traffic.

11. (Previously Presented) The network system of Claim 9, and further comprising a plurality of customer premises equipment (CPE) edge routers each coupled to a respective one of said plurality of ingress routers.

12. (Currently Amended) The network system of Claim 9, and further comprising a customer premises equipment (CPE) edge router to the access link, said CPE edge router

having a physical port coupled to said access link, said physical port implementing a first logical port for intra-VPN traffic and a second logical port for extra-VPN traffic.

13. (Canceled)

14. (Currently Amended) The network system of Claim 9, wherein at least one of said plurality of ingress routers implements a plurality of tunnels that logically partition intra-VPN and extra-VPN traffic, wherein said one or more egress routers provide a plurality of different qualities of services to said intra-VPN traffic.

15. (Canceled)

16. (Previously Presented) A method providing a virtual private network (VPN), said method comprising:

in an access network including the access link, providing a first logical connection for intra-VPN traffic from sources within the VPN and a second logical connection for extra-VPN traffic from sources outside the VPN;

communicating, from a plurality of ingress routers to one or more egress routers, intra-VPN and extra-VPN traffic destined for a destination host belonging to the VPN, wherein said intra-VPN traffic and said extra-VPN traffic are transmitted utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic, wherein intra-VPN traffic is given precedence over extra-VPN traffic by assigning a higher priority to the first access logical connection;

transmitting intra-VPN traffic from said one or more egress routers to the destination host via the first logical connection, and transmitting all extra-VPN traffic from said one or more egress routers to the destination host via the second logical connection, such that intra-VPN traffic and extra-VPN traffic are logically separated into different paths, whereby denial of service attacks on said access link originating from sources outside the VPN are prevented.

17. (Previously Presented) The method of Claim 16, wherein a Differentiated Services protocol is used to logically partition the intra-VPN traffic and the extra-VPN traffic using a differentiated services protocol to mark correspondingly the intra-VPN traffic and the extra-VPN traffic.

18. (Original) The method of Claim 16, wherein a customer premises equipment (CPE) edge router is coupled between said access network and said destination host, said method further comprising:

at a physical port of the CPE edge router coupled to the access link, providing first and second logical ports; and

receiving intra-VPN traffic at the first logical port, and receiving extra-VPN traffic at the second logical port.

19. (Previously Presented) The method of Claim 16, and further comprising logically partitioning intra-VPN and extra-VPN traffic by at least one of said plurality of ingress routers utilizing a plurality of tunnels.

20. (Previously Presented) The method of Claim 16, and further comprising said one or more egress routers providing a plurality of different qualities of services to said intra-VPN traffic.

21. (Previously Presented) A method for providing a virtual private network (VPN), the method comprising:

assigning a first priority level to intra-VPN traffic flowing from sources included in the VPN;

assigning a second priority level to extra-VPN traffic flowing from sources outside the VPN;

granting, to traffic having the first priority level at the access link, precedence of access to a destination host belonging to the VPN over traffic having the second priority level; and

transmitting the intra-VPN traffic from one or more egress routers to the destination host via a first logical connection, and transmitting all extra-VPN traffic from said one or more egress routers to the destination host via a second logical connection, such that intra-VPN traffic and extra-VPN traffic are logically separated into different paths, whereby denial of service attacks on said access link originating from sources outside the VPN are prevented.

22. (Previously Presented) A method of communicating, comprising:

receiving a packet that is destined to a host within a virtual private network;

determining whether the packet is originated within the virtual private network or external to the virtual private network; and

forwarding the packet to the host over a first logical path or a second logical path based on the determination, wherein the first logical path is designated for traffic originating within the virtual private network and the second logical path is designated for traffic

originating externally to the virtual private network, wherein the packet forwarded over the first logical path is given precedence over packets forwarded over the second logical path by assigning a higher priority to the first logical path.

23. (Previously Presented) The method of Claim 22, wherein the packet is an Internet Protocol (IP) packet, and the steps of receiving, determining and forwarding are performed at a customer premises router configured to process the IP packet.

24. (Previously Presented) The method of Claim 22, wherein the packet over the first logical path is marked as a higher priority than the second logical path using a differentiated services protocol.

25. (New) The network system of Claim 6, wherein said physical port comprises a Wide Area Network (WAN) physical port.

26. (New) The network system of Claim 25, wherein the WAN physical port is configured to employ a scheduler to multiplex packets from said first and second logical ports onto a transmission medium of said access network and to forward packets received from said access network to the first and second logical ports.

27. (New) The network system of Claim 4, wherein packets received by a port of the CPE edge router pass through a classifier configured to determine, by reference to a table, how each packet will be handled by the CPE edge router.

28. (New) The network system of Claim 7, wherein the plurality of tunnels are implemented utilizing one of IP-over-IP tunnel, a Generic Routing Encapsulation (GRE) tunnel, an Internet Protocol Security (IPSec) operated in tunnel mode, a set of stacked Multi-Protocol Label Switching (MPLS) labels, a Layer 2 Tunneling Protocol (L2TP), and a null tunnel.